544,172

Rec'd PCT/PTO 02 AUG 2005

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

10/544172

(43) International Publication Date
26 August 2004 (26.08.2004)

PCT

(10) International Publication Number
WO 2004/073234 A2

(51) International Patent Classification⁷: H04L

(21) International Application Number: PCT/US2004/003299

(22) International Filing Date: 5 February 2004 (05.02.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/445,805 7 February 2003 (07.02.2003) US

(71) Applicant (*for all designated States except US*): **MAGIQ TECHNOLOGIES, INC.** [US/US]; 275 Seventh Avenue, 26th Floor, New York, NY 10001 (US).

(72) Inventors; and

(75) Inventors/Applicants (*for US only*): **BERZANSKIS, Audrius** [LT/US]; 7 Saint Mary Road, Cambridge, MA 02139 (US). **TRIFONOV, Alexei** [RU/US]; 69 Park Drive, Apt. 8, Boston, MA 02215 (US).

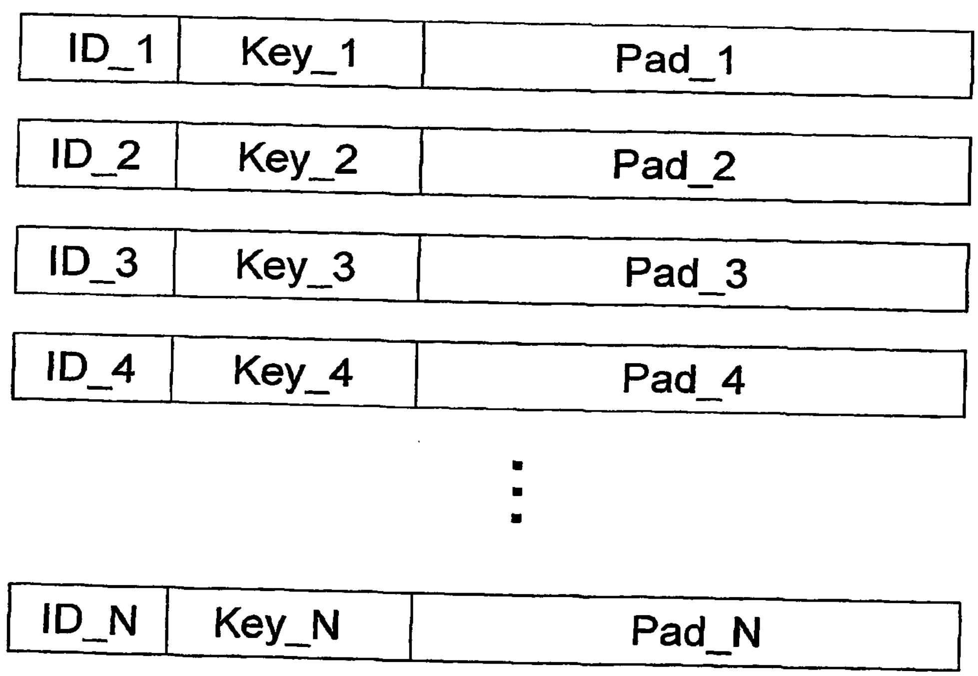
(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: KEY EXPANSION FOR QKD



(57) Abstract: A method of encrypting information using an encryption pad based on keys exchanged between quantum key distribution (QKD) stations is disclosed. The method includes establishing raw keys between two stations using QKD, processing the keys to establish a plurality of matching privacy amplified keys at each station and buffering the keys in a shared key schedule. The method also includes the option of expanding one or more of the keys in the shared key schedule using a stream cipher to create a supply of expanded keys that serve as pads for one-time-pad encryption.

WO 2004/073234 A2